UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/573,367	02/23/2007	Philippe Guillot	17250/017001	2146

22511 7590 11/30/2011

OSHA LIANG L.L.P.
TWO HOUSTON CENTER
909 FANNIN, SUITE 3500
HOUSTON, TX 77010

EXAMINER	
TOLENTINO, RODERICK	

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
11/30/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@oshaliang.com
hathaway@oshaliang.com
kennedy@oshaliang.com

Office Action Summary	Application No.	Applicant(s)	
	10/573,367	GUILLOT ET AL.	
	Examiner	Art Unit	
	RODERICK TOLENTINO	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09/2/2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13 and 15-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13 and 15-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 March 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 13 and 20 are pending.

Response to Arguments

2. Applicant's arguments filed 09/02/2011 have been fully considered but they are not persuasive.

3. Applicant argues that Maillard in view of Kirkland fail to disclose, teach or even suggest "selecting a first key, the first key being unique in the broadcasting network and being dedicated to a single device in the broadcasting network; assigning the first key to the decoder, wherein the decoder and the portable security module form a first receiving decoding system among a plurality of receiving decoding systems in the broadcasting network, wherein each receiving decoding system is configured to descramble scrambled audiovisual data received via the broadcasting network; determining a second key according to the first key, such that a combination of the first key and the second key is congruent to a pairing system key, wherein the pairing system key is common to each receiving decoding system and allows for decryption of encrypted control data, the encrypted control data being identical for each receiving decoding system; assigning the second key to the portable security module to obtain a pairing of the decoder and the portable security module," regarding claim 1. Examiner respectfully disagrees. As per claims 1 and 15, Maillard discloses assigning the first key to the decoder, wherein the decoder and the portable security module form a first receiving decoding system among a plurality of receiving decoding systems in the

broadcasting network, wherein each receiving decoding system is configured to descramble scrambled audiovisual data received via the broadcasting network (Maillard, Col. 2 Lines 13 – 20, key for decoding), determining a second key according to the first key , such that a combination of the first key and the second key is congruent to a pairing system key, wherein the pairing system key is common to each receiving decoding system and allows for decryption of encrypted control data he encrypted control data being identical for each receiving decoding system (Maillard, Col. 8 Lines 55 – 63, key pair for decoder and smart card), assigning and the second key to the portable security module to obtain a pairing of the decoder and the portable security module (Maillard, Col. 1 Lines 57 – 64, portable decoder) but fails to teach selecting a first key, the first key being unique in the broadcasting network and being dedicated to a single device in the broadcasting network. However, in an analogous Kirkland teaches selecting a first key, the first key being unique in the broadcasting network and being dedicated to a single device in the broadcasting network (Kirkland, Paragraph 0005, key pair unique between the devices).

4. Maillard teaches on Col. 2 Lines 13 – 20, a decoder with an encryption key, the decoder which is used to descramble data which is further shown on Col. 1 Lines 57 – 64. Maillard also further explains on Col. 8 Lines 47 – 54, which a key is provided to the decoder for descrambling of data. Thus Maillard teaches the recited limitation of "assigning the first key to the decoder, wherein the decoder and the portable security module form a first receiving decoding system among a plurality of receiving decoding systems in the broadcasting network, wherein each receiving decoding system is

configured to descramble scrambled audiovisual data received via the broadcasting network," since a key is provided to a decoder device used to descramble data.

5. Maillard teaches on Col. 8 Lines 55 – 63, a public/private key pairing system which is used which reads on the limitation of "determining a second key according to the first key, such that a combination of the first key and the second key is congruent to a pairing system key, wherein the pairing system key is common to each receiving decoding system and allows for decryption of encrypted control data, the encrypted control data being identical for each receiving decoding system." The public key is known by all and each decoder will have its own private key in order to descramble a control word which is taught on Col. 7 Lines 12 – 25. But in general it is by definition that the public is known by all devices and is common amongst the. A key pair is by definition means that the pair are congruent to each other, so the applicant's arguments are moot on this point. Applicant argues on page 10 of the response that Maillard does not validate a combination of the encryption key of the portable security module and the decryption key of the decoder by checking the congruence of the combination. This argument is moot since the Applicant is not arguing a limitation that is recited in the claim. No where in the claim is there a recited validation step. All arguments regarding this validation must be seen as moot.

6. Maillard teaches on Col. 1 Lines 57 – 64, that the portable decoder is assigned and as described above Maillard teaches the use of public/private key pairing for decoders to descramble data.

7. Kirkland teaches on paragraph 0005, how the key pair is unique to a device and a system and thus teaching the limitation that "the first key is unique in the broadcasting network and being dedicated to a single device in the broadcasting network." A key pair is by definition unique to the owner being the device and the network.

8. Applicant also argues that Maillard in view of Kirkland fail to teach a broadcast network however, clearly on Col. 4 Lines 6 – 13, the transmission of the broadcast, teaching the limitations of a broadcast network.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1 – 7, 11 – 13, 15, 16, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maillard et al. U.S. Patent No. (6,286,103) in view of Kirkland U.S. PG-Publication No. (2004/0264700).

11. As per claims 1 and 15, Maillard discloses assigning the first key to the decoder, wherein the decoder and the portable security module form a first receiving decoding system among a plurality of receiving decoding systems in the broadcasting network, wherein each receiving decoding system is configured to descramble scrambled

audiovisual data received via the broadcasting network (Maillard, Col. 2 Lines 13 – 20, key for decoding), determining a second key according to the first key , such that a combination of the first key and the second key is congruent to a pairing system key, wherein the pairing system key is common to each receiving decoding system and allows for decryption of encrypted control data he encrypted control data being identical for each receiving decoding system (Maillard, Col. 8 Lines 55 – 63, key pair for decoder and smart card), assigning and the second key to the portable security module to obtain a pairing of the decoder and the portable security module (Maillard, Col. 1 Lines 57 – 64, portable decoder) but fails to teach selecting a first key, the first key being unique in the broadcasting network and being dedicated to a single device in the broadcasting network. However, in an analogous Kirkland teaches selecting a first key, the first key being unique in the broadcasting network and being dedicated to a single device in the broadcasting network (Kirkland, Paragraph 0005, key pair unique between the devices).

12. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Kirkland's wireless bridge for secure dedicated connection to a network with Maillard's apparatus for encrypted data stream transmission because it offers the advantage of preventing unauthorized users from transmitting and receiving wireless signals. (Kirkland, Paragraph 0004).

13. As per claim 2, Maillard discloses the control data enables to descramble the scrambled audiovisual information, the method further comprising: receiving at the first decoding system the encrypted control data; using the first key at the first element and

using the second key at the second element to decrypt the encrypted control data (Maillard, Col. 1 Lines 57 – 64, decryption of data).

14. As per claim 3, Maillard discloses the control data is a control word, the audiovisual information being scrambled using the control word (Maillard, Col. 6 Lines 25 – 43, Control Word).

15. As per claim 4, Maillard discloses the control data is an Entitlement Control Message (ECM) comprising a control word, the audiovisual information being scrambled using the control word (Maillard, Col. 6 Lines 44 – 54, ECM).

16. As per claim 5, Maillard discloses the control data is an exploitation key, the exploitation key enabling to decode a control word, the audiovisual information being scrambled using the control word (Maillard, Col. 8 Lines 13 – 24, decrypted Control word).

17. As per claim 6, Maillard discloses the control data is an Entitlement Management Message (EMM) comprising an exploitation key enabling to decode a control word, the audiovisual information being scrambled using the control word (Maillard, Col. 7 Lines 1 – 11, encrypted EMMs).

18. As per claim 11, Maillard discloses the encrypted information is the scrambled audiovisual information (Maillard, Col. 8 Lines 13 – 24, Scrambled audiovisual).

19. As per claim 12, Maillard discloses the encrypted information is a control word, the audiovisual information being scrambled using the control word (Maillard, Col. 8 Lines 13 – 24, Scrambled audiovisual).

20. As per claim 13, Maillard discloses respectively attributing the first key and the second key at least to a third element and a fourth element forming a second decoding system distinct from the first decoding system (Maillard, Col. 2 Lines 13 – 20, key for decoding).

21. As per claim 16, Maillard discloses receiving means to receive the broadcasted encrypted control data; a pair of decryptions comprising a first decryption and a second decryption respectively located in the first element and the second element, the pair of decryptions enabling to decrypt the broadcasted encrypted control data using the first key and the second key (Maillard, Col. 8 Lines 55 – 63, key pair for decoder and smart card).

22. As per claim 19, Maillard discloses the control data is a control word, the audiovisual information being scrambled using the control word (Maillard, Col. 8 Lines 13 – 24, Scrambled audiovisual).

23. As per claim 20, Maillard discloses the control data is an exploitation key, the exploitation key enabling to decode a control word, the audiovisual information being scrambled using the control word (Maillard, Col. 8 Lines 13 – 24, Scrambled audiovisual).

24. As per claim 21, Maillard discloses the first element is a decoder; the second element is a portable security module (Maillard, Col. 1 Lines 57 – 64, portable decoder).

25. Claims 7 – 10, 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maillard et al. U.S. Patent No. (6,286,103) and Kirkland U.S. PG-

Publication No. (2004/0264700) in view of Kocher et al. U.S. PG-Publication No. (2001/0002486).

26. As per claim 7, Maillard fails to teach selecting a first prime number p and a second prime number q; calculating a modulus number n as being equal to a product of the first prime number p and the second prime number q; selecting an encrypting key e as being smaller to the modulus number and as being prime with a function of the first prime number p and the second prime number q; determine a private key as being equal to an inverse of the encrypting key modulus the function of the first prime number p and the second prime number q; selecting the first key and the second key such that a product of the first key and the second key equals the private key modulo the function of the first prime number p and the second prime number q; erasing the first prime number p and the second prime number q. However, in an analogous art Kocher teaches selecting a first prime number p and a second prime number q; calculating a modulus number n as being equal to a product of the first prime number p and the second prime number q; selecting an encrypting key e as being smaller to the modulus number and as being prime with a function of the first prime number p and the second prime number q; determine a private key as being equal to an inverse of the encrypting key modulus the function of the first prime number p and the second prime number q; selecting the first key and the second key such that a product of the first key and the second key equals the private key modulo the function of the first prime number p and the second prime number q; erasing the first prime number p and the second prime number q (Kocher, Paragraph 0076, RSA).

27. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Kocher's leak-resistant cryptographic method in view of Maillard's apparatus for encrypted data stream transmission because it offers the advantage of preventing attackers from accessing keys (Kocher, Paragraph 0003).

28. As per claim 8, Maillard as modified teaches receiving at each receiving decoding system a message comprising the encrypted control data; decrypting the encrypted control data using the first key at the first element and the second key at the second element (Maillard, Col. 1 Lines 57 – 64, decryption of data).

29. As per claim 9, Maillard as modified teaches the encrypted control data is decrypted using a discrete logarithms algorithm, the method further comprising: selecting a prime number q; selecting a primitive root of the prime number g; and wherein a product of the first key and the second key equals a private key modulo the prime number (Kocher, Paragraph 0076, RSA).

30. As per claim 10, Maillard as modified teaches receiving at each receiving decoding system a message comprising an encrypted information encrypted with a cession key, the message also comprising the primitive root of the prime number g power a random number k; using the first key at the first element and using the second key at the second element to calculate the cession key from the prime number power the random number k; decrypting the encrypted information using the cession key (Kocher, Paragraph 0076, RSA).

31. As per claim 17, Maillard fails to teach wherein the broadcasted encrypted control data is decrypted using a discrete logarithm algorithm. However, in an

analogous art Kocher teaches the broadcasted encrypted control data is decrypted using a discrete logarithm algorithm (Kocher, Paragraph 0076, RSA).

32. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Kocher's leak-resistant cryptographic method in view of Maillard's apparatus for encrypted data stream transmission because it offers the advantage of preventing attackers from accessing keys (Kocher, Paragraph 003).

33. As per claim 18, Maillard as modified teaches the broadcasted encrypted control data is decrypted using a RSA algorithm (Kocher, Paragraph 0076, RSA).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to RODERICK TOLENTINO whose telephone number is

(571)272-2661. The examiner can normally be reached on Monday - Friday 9am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Roderick Tolentino
Examiner
Art Unit 2439

Roderick Tolentino
/R. T./
Examiner, Art Unit 2439

/Edan Orgad/
Supervisory Patent Examiner, Art Unit 2439